

DEFENSE MESSAGE SYSTEM (DMS)



DISA ACAT IAM Program

Total Number of Systems:	700+ sites
Total Program Cost (TY\$):	\$409M
Life-Cycle Cost (TY\$):	\$5B
Full-rate production:	2QFY98

Prime Contractor

Lockheed Martin Federal Systems

SYSTEM DESCRIPTION & CONTRIBUTION TO JOINT VISION 2020

The Defense Message System (DMS) contributes to *information superiority* and *interoperability* to achieve **Joint Vision 2020** by enabling anyone in DoD to exchange messages with anyone else in DoD using a secure, accountable, and reliable writer-to-reader messaging system. **Full dimensional protection** is provided by the National Security Agency's Multi-level Information System Security Initiative technology, employing Fortezza cards for personnel identification and encryption services and other Information Assurance protections. DMS must also provide ordinary e-mail ("individual" messaging) by handling both commercial and classified messages. DMS is intended to reduce the cost and manpower demands of the legacy "organizational" messaging system based on 1960s technology—the Automatic Digital Network (AUTODIN). To replace AUTODIN, DMS must be implemented in over 40,000 organizations at over 700 sites worldwide and support message exchanges with tactical forces, allies, other federal government users, and defense contractors. By employing the latest commercial technology, supporting Allied Communications Publications (ACP) 120, and operating on Defense Information Infrastructure (DII) computers and communications backbone, the DMS program will ensure *innovation*. While today's security needs require using the international X.400 messaging

standard and X.500 directory services standard, the DMS program anticipates development of adequate security and military features to be implemented in the more common Internet e-mail standards.

BACKGROUND INFORMATION

The Defense Information Systems Agency began the DMS program in 1989. By 1992, the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence issued a policy mandating the transition to, and use of, DMS compliant systems. In March 1995, additional policy guidance imposed a moratorium on the acquisition of non-DMS compliant electronic messaging systems. Since the August 1997 IOT&E of release 1.0, DMS has continued to improve through two Operational Assessments (OA) in 1998 and 1999. AUTODIN has been steadily downsized to a few message centers called DMS Transition Hubs (DTHs). An OT&E of DMS Release 2.1 showed marked improvement, with all five functional COIs resolved satisfactorily. The security COI was not resolved satisfactorily because Information Warfare penetration testing revealed security deficiencies. DOT&E's independent assessment found DMS 2.1 to be not operationally suitable because a typical system administrator was poorly equipped to install, maintain, troubleshoot, and ensure security configuration of the system. DMS 2.2 consolidates many system upgrades and fixes and introduces an Automated Message Handling System (AMHS) capability necessary for CINC implementation of DMS messaging. Full implementation of DMS requires replacing AUTODIN, supporting ACP 120 message standards, and implementing tactical and intelligence elements through Service and agency programs. These efforts will take several years, involving additional DMS releases and operational tests. For the interim, DTHs support the residual AUTODIN traffic for strategic and some other critical missions.

TEST & EVALUATION ACTIVITY

In spring 2000, the Air Force Information Warfare Center conducted security tests on site-level DMS configurations and the Regional Node and Operations and Security Center (RNOSC) in Columbus, OH. In the fall 2000, the Joint Interoperability Test Command led a multi-Service test team conducting an OA of DMS 2.2, with a Quicklook briefing on December 13. The next scheduled release, DMS 3.0, is supposed to implement the ACP 120 standard that requires interdependent modifications to most DMS components. DMS 3.0 will require a full OT&E.

TEST & EVALUATION ASSESSMENT

The spring follow up security tests again revealed that site system administrators had failed to protect all elements, and that the RNOSC had a vulnerable directory server which could be exploited to conduct a system-wide denial of service attack. During the DMS 2.2 OA, security testers again penetrated each of the five test sites, the RNOSC, and other infrastructure nodes. Weak passwords, clear-text scripts/files with sensitive information, and lax procedures continued to cause most vulnerabilities. RNOSC security is hampered by lack of a firewall. Windows environments within a site domain rely on trust relationships across that domain, and thus the DMS environment is dependent on the level of security maintained in other systems operating within the same domain as DMS. Several penetrations into the DMS platforms were achieved by exploiting these trust relationships.

For the OA of DMS 2.2, a DMS-interface was required to be installed for the AMHS. Several configuration issues were discovered and modifications were implemented immediately prior to the OA. The Norfolk site completed a major re-design just prior to the OA. Other configuration problems were

discovered either late in the preparation of the OA, or after OA start. A security patch installed in the mail list agents induced failure in that product. Messaging between DMS and legacy and Allied users suffered due to missing routing information and procedural problems at the Ft. Detrick DTH. Errors in implementing important change notifications are indicative of system immaturity and lack of attention to detail by system administrators. This is exacerbated by documentation complexity and reliance on manual processes. While configuration errors caused many problems, the difficulty and delay in finding and fixing problems is a more serious concern. System administrators were not sufficiently skilled or equipped for troubleshooting, or capturing and forwarding information for further diagnosis by the Help Desk system. At the time of this publication, DMS 2.2 is currently assessed as not operationally effective and not suitable. However, the PM has implemented a plan to resolve the issues found in the OA, and upon resolution, DMS 2.2 will undergo follow-on operational assessment during 2QFY01.

CONCLUSIONS, RECOMMENDATIONS AND LESSONS LEARNED

The DII is outside of the scope of the DMS program's control and remains a source of performance uncertainty. Published analyses of the traffic fluctuations of the worldwide Internet suggest that the military DII Internets will also experience severe variability and outages, which no one currently knows how to manage or prevent. These prospects call for broader, more integrated operational tests with embedded security evaluations to evaluate the DII and all of the interoperable systems it supports. Advanced forms of modeling appropriate for representing Internet traffic should also be applied to assessments of DMS and the DII under wartime stresses.

The DMS commercial competition acquisition strategy leads to a proliferation of computer platforms and operating systems, and complicates testing and implementation. Military-unique features, such as strong security protection and non-deniability of message receipt, require modifications of commercial software. Rapidly changing commercial practices require that DMS remain current through frequent modifications. Operational test measures revealed most of these effects of complexity, as most sites became operational with 40 percent of user-accounts being implemented.

The ability to harden the DMS in laboratory shows that repeated failures to fix security vulnerabilities at fielded sites is mostly a result of the inability of local administrators to check whether they have achieved or otherwise compromised a secure posture. This suggests a combined need for better security training, more discipline and attention to detail, command focus, and better automated tools to help assess the overall system security configuration. As DMS extends below the joint level into tactical, allied, intelligence, strategic, diplomatic, and other applications, the security overhead burden becomes ever more difficult and error prone. In the tactical environment, managing a Public Key Infrastructure that requires updating every 56 days is challenging. Demands for security by intelligence organizations, or reliability by strategic organizations, challenge the compromises necessary to stay current with commercial technology. High-assurance guards for passing messages between adjacent security levels can be tailored to local organizational needs, but local security policies may not be adequate for other programs or organizations sharing the same networks. For these and similar reasons, DMS is evolving a complex set of operational and security practices that will be difficult to teach, and for which combinations of conditions will be difficult to anticipate and test. The complexity of installing DMS and maintaining DMS configurations is error prone and requires attention to detail. Operational tests only marginally exercise these tasks, and automated tools under development were not ready for DMS 2.2. This OA was especially valuable in demonstrating the importance of training, procedures, and automated tools for system administrators. The diversity of site configurations and operational needs, combined with technology upgrades, pose design and testing challenges. We recommend intensive development and OT&E of these critical tools and procedures.

